REMARKS

Claims 1-2, 6-12 and 15-17 of the patent application were presented for examination. In the Office Action of June 5, 2008, claims 1-2, 6-12 and 15-17 were rejected. The claims, as amended, are listed above. No new matter has been added. Accordingly, claims 1-2, 6-12 and 15-17 are now pending for examination.

Applicant requests entry of the above amendments and reconsideration of allowance of the claims. Applicant responds to the rejections as follows:

Claim Objections

Claims 6-12 and 17 were objected to because of informalities. Specifically, Examiner noted that the terms "first register" and "second register" were not used in a manner consistent with the Specification.

Applicant confirms that the designations of "first" and "second" are merely arbitrary distinctions that do not allude to a required sequence. Thus, the designations need to be exactly in the same sequence as described in the Specification.

Claim 6 was further objected to because of the grammatical misuse of the term "identity."

In response, claim 6 has been amended to obviate the grammatical error.

Applicant respectfully requests withdrawal of the objections.

Claim Rejections Under 35 U.S.C. §112(2)

Claims 1, 2, 6-12 and 15-17 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject mater which Applicant regards as the invention. Specifically, Examiner asserted that the claims were unclear as to whether identities of the boot sources were being compared, or if bytes of the boot sources were being compared.

As amended, the claims more clearly specify that identification information associated with the boot sources are being compared. Thus, Applicant respectfully requests withdrawal of the rejection.

Claim Rejections Under 35 U.S.C. §103(a)

Claims 1-2, 6-8, 10-12, 16 and 17 are rejected under 35 USC 103(a) as being unpatentable over Grawrock (US Patent No. 6,678,833) in view of Jablon (US Patent No. 5,421,006).

Claims 9 and 15 are rejected under 35 USC 103(a) as being unpatentable over Grawrock, in view of Jablon, and further in view of Davis et al. (U.S. Patent No. 6,401,208)("Davis").

Applicant respectfully traverses the rejections.

Present Invention

For ease of examination, claim 1, as amended, is reproduced below. Independent claim 1 includes limitations representative of independent claim 6. Specifically, claim 1 is directed to a method for verifying a boot source in a computer system having a processor. The method comprises:

storing a trusted boot source in a first register from a peripheral connector, the trusted boot source having identification information, the first register comprising a write-once register;

determining identification information of an actual boot source used by the processor each time the computer system boots including examining a location of a predetermined number of instructions initially executed during boot up; and

comparing the identification information of the actual boot source against the identification information of the trusted boot source.

Prior Art

Grawrock generally discloses an integrated circuit devices with a trusted platform module and a blot block memory unit (Abstract). More particularly, Grawrock discloses that a boot block identifier is calculated for each start-up of the platform from boot information (3:62-63). Boot services can include a root of trust such as a boot block code executed at the start of the initialization process of the platform to locate, load and pass control of the BIOS (3:41-44). Thus, Grawrock discloses calculating boot block information.

Jablon generally discloses a method for reliably assessing the integrity of a computer system's software to prevent execution of corrupted programs at the time of system initialization.

Davis generally discloses a cryptographic device implemented in communication with a host processor to prevent the host processor from performing a standard boot-up procedure until a BIOS is authenticated.

Arguments

However, Grawrock, Jablon and/ or Davis, either alone or in combination, fail to teach or suggest the invention as recited in claim 1, as discussed below. Therefore, Applicant submits that claim 1, and all related claims, are patentable over the applied references. Similarly, claim 6, and all related claims, are patentable for at least the same reasons as claim 1.

A. *Grawrock, Jablon and Davis Each Fail to Teach or Suggest Storing a Trusted Boot Source in a First Register from a Peripheral Connector, the First Register Comprising a Write-Once Register*

Claim 1 recites storing a trusted boot source in a first register from a peripheral connector (e.g., a PCI connector). The first register of claim 1 comprises a write-once register. Advantageously, the trusted boot source can still be programmed during manufacturing using the peripheral connector, but protected from an unscrupulous boot source loaded from the peripheral connector at a later time.

Meanwhile, Grawrock discloses calculating a boot block identifier for a first start-up and retains the identifier in a non-volatile memory for subsequent use during later start-ups

(Grawrock 3:63-67). The boot block identifier of Grawrock is just information about the boot block, not the boot block itself. Grawrock is silent regarding any techniques for programming the boot block.

Although Jablon discloses a BIOS residing in a read only memory (Jablon 11:57), Jablon does not disclose how the BIOS is originally programmed. Also, the latch disclosed by Jablon can be closed to prevent modification of the BIOS (Jablon 50-60), but the latch can also be opened to be modified, so the latch is not a write-once register as claimed.

Davis, while disclosing that firmware is pre-programmed, provides no details as to how the programming occurs. Thus, Davis fails to disclose the specificity of using a peripheral connector for programming.

Consequentially, neither Grawrock, Jablon or Davis discloses a write-once register programmed through a peripheral connector, as recited in claim 1.

B. *Grawrock, Jablon and Davis Each Fail to Teach or Suggest Comparing the Identification Information to Prevent an Unscrupulous Boot Source from being Loaded Through the Peripheral Connector*

Claim 1 recites comparing the identification information of the trusted boot source against the actual boot source. Because a boot source can be loaded through the peripheral connector, the comparison can identify an unwanted boot source.

Grawrock fails to disclose comparing boot sources as acknowledged by Examiner (OA, p. 5).

While Jablon discloses verifying a boot record program when loading against when BIOS runs the boot record program, the technique of Jablon provides no protection against the first loaded boot record program. As a result, the first loaded boot program can be unscrupulous and cannot be identified as such, as in claim 1.

Davis fails to disclose comparing boot sources.

C. *Potential Combination of Grawrock, Jablon and Davis, or other Prior Art*

As discussed, neither Grawrock, Jablon or Davis discloses the elements of claim 1, either alone or combined. However, assuming arguendo, that one of the references could be interpreted as allowing programming using the peripheral connector, a proper rejection must also prevent an unscrupulous boot source loaded from the same peripheral connector, as is recited in claim 1.

CONCLUSION

On the basis of the above remarks, reconsideration and allowance of the claims is believed to be warranted and such action is respectfully requested. If Examiner has any questions or comments, Examiner is respectfully requested to contact the undersigned at the number listed below.

Respectfully submitted,

SAWYER LAW GROUP LLP

September 30, 2008

/Joseph A. Sawyer, Jr/
Joseph A. Sawyer, Jr.
Reg. No. 30,801

Customer Number: 29141
(650) 493-4540
(650) 493-4549